# PATENT COOPERATION TREATY



PCT

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

## WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

| | |
|---|---|
| Applicant's or agent's file reference<br>see form PCT/ISA/220 | Date of mailing<br>*(day/month/year)* see form PCT/ISA/210 (second sheet)<br>**FOR FURTHER ACTION**<br>See paragraph 2 below |

| International application No. | International filing date *(day/month/year)* | Priority date *(day/month/year)* |
|---|---|---|
| PCT/EP2004/012226 | 28.10.2004 | 29.10.2003 |

International Patent Classification (IPC) or both national classification and IPC
H04L9/08

Applicant
ARGELCOM LIMITED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Cretaine, P

Telephone No. +49 89 2399-8828

# WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/EP2004/012226

## Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

# WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/EP2004/012226

## Box No. II Priority

1. ☒ The following document has not been furnished:

   ☒ copy of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(a)).

   ☐ translation of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(b)).

   Consequently it has not been possible to consider the validity of the priority claim. This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

3. ☐ It has not been possible to consider the validity of the priority claim because a copy of the priority document was not available to the ISA at the time that the search was conducted (Rule 17.1). This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

4. Additional observations, if necessary:

## Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

| | | | |
|---|---|---|---|
| Novelty (N) | Yes: | Claims | 1-8 |
| | No: | Claims | |
| Inventive step (IS) | Yes: | Claims | 1-8 |
| | No: | Claims | |
| Industrial applicability (IA) | Yes: | Claims | 1-8 |
| | No: | Claims | |

2. Citations and explanations

**see separate sheet**

**Re Item V**

**Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

Reference is made to the following document:

D1 = B.PRENEEL ET AL.: NESSIE SECURITY REPORT, PAGES I-VII, 178-201, 19 February 2003 (2003-02-19), XP002316503

**Prior art:**

The document D1 is regarded as being the closest prior art to the subject-matter of **claim 1**, and shows (see paragraphs 6.3.1, 6.3.3) a secure communication system using a key encapsulation mechanism (KEM) and a data encapsulation mechanism (DEM): the key encapsulation mechanism (KEM) utilises the receiving location's public key and a random seed to provide a symmetric session key, and provides an encryption of the session key under the receiving location's public key; the data encapsulation mechanism then uses the session key to symmetrically encrypt the message to be transmitted from the sending location to the receiving location. The sending location transmits to the receiving location both the encrypted session key and the encrypted message. The receiving location recovers the session key using its private key and then uses the session key to recover the message.

**Novelty:**

The subject-matter of claim 1 differs essentially from this known system in that the claimed system comprises a plurality of receiving locations, each associated with a private/public key pair: at the sending location, a plurality of encryptions of the session key are performed, each with the public key of sending location, and sent together to each of the receiving locations; the message is sent encrypted with the session key to each of the receiving locations; each of the receiving location uses its own private key to decrypt the encrypted version of the session key corresponding to its own public key.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

**Inventive step:**

The problem to be solved by the present invention may be regarded as how to perform an efficient multicast of a message in a KEM-DEM system.

The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:
the skilled person, starting from the known point-to-point KEM-DEM method, will naturally use a KEM-DEM session between the sending location and each one of the receiving location, thereby providing a session key for each of the receiving location and sending the message encrypted with respective session keys to each one of the plurality of receiving locations.
Nothing in the prior art documents would lead the skilled person to use the particular procedure of claim 1 with a single session key and a plurality of encryptions of this session key.

Therefore claim 1 meets the requirements of Article 33(3) PCT.

Independent **claim 5** contains the same features combination as claim 1 in terms of a method claim. Therefore claim 5 meets the requirements of Article 33(3) PCT.

Independent **claim 2** relates to an alternative of the invention wherein the message is used as input to the system instead of the random number generator, the message being then encrypted with each the public keys of the receiving location and being recovered at each of the receiving locations.
The particular combination of features of claim 2, relating to a multicast KEM-DEM procedure with the message itself being used as input to the KEM, is not disclosed in or suggested by the documents of the search report.
Therefore claim 2 meets the requirements of Article 33(3) PCT.

Independent **claim 6** contains the same features combination as claim 2 in terms of a method claim. Therefore claim 6 meets the requirements of Article 33(3) PCT.

Claim 3, 4, 6 and 8 are dependent on claims 2 or 6 and as such also meet the requirements of the PCT with respect to novelty and inventive step.